

JC10 Rec'd 30 OCT 2001

FORM PTO-1390 (REV 10-94)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		DOCKET #: 4925-158PUS
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371				
				U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 10 009658
INTERNATIONAL APPLICATION NO PCT/FI00/00421		INTERNATIONAL FILING DATE 11 May 2000		PRIORITY DATE CLAIMED 11 May 1999
TITLE OF INVENTION Integrity Protection Method For Radio Network Signaling				
APPLICANT(S) FOR DO/EO/US Valtteri NIEMI; Jaakko RAJANIEMI; Ahti MUHONEN				
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:				
<ol style="list-style-type: none"> 1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371 3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1). 4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date. 5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2)) <ol style="list-style-type: none"> a. <input checked="" type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> has been transmitted by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US) 6. <input type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)). 7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)) <ol style="list-style-type: none"> a. <input checked="" type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). (see Reply to Written Opinion). b. <input type="checkbox"/> have been transmitted by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input type="checkbox"/> have not been made and will not be made. 8. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). 9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). Unexecuted 10. <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)). <p>Items 11. to 16. Below concern other document(s) or information included:</p> <ol style="list-style-type: none"> 11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 12. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. 13. <input type="checkbox"/> A FIRST preliminary amendment. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. 14. <input checked="" type="checkbox"/> A substitute specification. 15. <input type="checkbox"/> A change of power of attorney and/or address letter. 16. <input checked="" type="checkbox"/> Other items or information (<i>specify</i>): PCT Publication Sheet, Int'l Preliminary Examination Report, Written Opinion, Reply to Written Opinion, Int'l Search Report, PCT Request, and PCT Demand 				

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)		INTERNATIONAL APPLICATION NO.		ATTORNEY'S DOCKET NUMBER	
10/005658		PCT/FI00/00421		4925-158PUS	
17.[x]The following fees are submitted:					
Basic National Fee (37 CFR 1.492(a)(1)-(5)):					
Search Report has been prepared by the EPO or JPO\$890.00					
International preliminary examination fee paid to USPTO (37 CFR 1.482).....\$710.00					
No international preliminary examination fee paid to USPTO (37 CFR 1.482)					
but international search fee paid to USPTO (37 CFR 1.445(a)(2)).....\$740.00					
Neither international preliminary examination fee (37 CFR 1.482)					
nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO\$1040.00					
International preliminary examination fee paid to USPTO (37 CFR 1.482)					
and all claims satisfied provisions of PCT Article 33(2)-(4)\$100.00					
ENTER APPROPRIATE BASIC FEE AMOUNT =				\$	890
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	8 - 20 =		x \$18.00	\$	
Independent Claims	1 - 3 =		x \$84.00	\$	
Multiple dependent claim(s) (if applicable)			+ \$280.00	\$	
TOTAL OF ABOVE CALCULATIONS =				\$	890
Reduction of 1/2 for filing by small entity, if applicable.				\$	
SUBTOTAL =				\$	890
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	
TOTAL NATIONAL FEE =				\$	890
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by the appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property				\$	
TOTAL FEES ENCLOSED				\$	890
Amount to be refunded:				\$	
charged:				\$	

- a. [x] One check in the amount of \$ 890 to cover the above fees is/are enclosed.
- b. ☐ Please charge my Deposit Account No. 03-2412 in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. [x] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 03-2412. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Michael C. Stuart
Cohen, Pontani, Lieberman & Pavane
551 Fifth Avenue, Suite 1210
New York, New York 10176

Michael C. Stuart
Registration Number: 35,698 October 30, 2001
Tel: (212) 687-2770

2/prts.

1

Integrity protection method for radio network signaling

TECHNICAL FIELD OF THE INVENTION

5 The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Particularly, the invention is directed to such a method as described in the preamble of Claim 1.

BACKGROUND OF THE INVENTION

10 All telecommunication is subject to the problem of how to make sure that the received information is sent by an authorized sender and not by somebody who is trying to masquerade as the sender. The problem is evident in cellular telecommunication systems, where the air interface presents an excellent platform for eavesdropping and replacing the contents of a transmission by using higher transmission levels, even from a distance. A basic solution to this problem is authentication of the communicating parties. An authentication process aims to
15 discover and check the identity of both of the communicating parties, so that each party receives information about the identity of the other party, and can trust the identity to a sufficient degree. Authentication is typically performed in a specific procedure at the beginning of the connection. However, this leaves room for unauthorized manipulation, insertion, and deletion of subsequent messages. Thus,
20 there is a need for separate authentication of each transmitted message. The latter task can be done by appending a message authentication code (MAC) to the message at the transmitting end, and checking the MAC value at the receiving end.

A MAC is typically a relatively short string of bits, which depends in some specified way on the message it protects and on a secret key known both by the sender and by
25 the recipient of the message. The secret key is generated and agreed typically in connection with the authentication procedure in the beginning of the connection. In some cases the algorithm that is used to calculate the MAC based on the secret key and the message is also secret but this is not usually the case.

The process of authentication of single messages is often called integrity protection.
30 To protect the integrity of signaling, the transmitting party computes a MAC value based on the message to be sent and the secret key using the specified algorithm, and sends the message with the MAC value. The receiving party recomputes a MAC value based on the message and the secret key according to the specified algorithm,

and compares the received MAC and the calculated MAC. If the two MAC values match, the recipient can trust that the message is intact and sent by the supposed party. One may note in passing, that integrity protection does not usually include protection of confidentiality of the transmitted messages.

5 Integrity protection schemes are not completely perfect. A third party can try to manipulate and succeed in manipulating a message transmitted between a first and a second party. There are two main alternative methods for forging a MAC value for a modified or a new messages, namely by obtaining the secret key first, and by trying directly without the secret key.

10 The secret key can be obtained by a third party basically in two ways:
 - by computing all possible keys until a key is found, which matches with data of observed message-MAC pairs, or by otherwise breaking the algorithm for producing MAC values; or
 - by directly capturing a stored or transmitted secret key.

15 The original communicating parties can prevent a third party from obtaining the secret key by using an algorithm that is cryptographically strong and which uses a long enough secret key to prevent exhaustive search of all keys, and using other security means for transmission and storage of secret keys.

A third party can try to disrupt messaging between the two parties without a secret
 20 key basically by guessing the correct MAC value, or by replaying of some earlier message transmitted between the two parties, for which message the correct MAC is known from the original transmission.

Correct guessing of the MAC value can be prevented by using long MAC values.
 The MAC value should be long enough to reduce the probability of guessing right to
 25 a sufficiently low level compared to the benefit gained by one successful forgery. For example, using a 32 bit MAC value reduces the probability of a correct guess to $1 / 4\,294\,967\,296$, which is small enough for most applications.

Obtaining a correct MAC value using the replay attack i.e. by replaying an earlier
 30 message can be prevented by introducing a varying parameter to the calculation of the MAC values. For example, a time stamp value, a sequence number, or a random number can be used as a further input to the MAC algorithm in addition to the secret integrity key and the message. The present invention is associated with this basic method. In the following, the prior art methods are described in more detail.

When using a time stamp value, each communicating party needs to have an access to a reliable clock in order to be able to calculate the MAC in the same way. The problem with this approach is the need of the reliable clock. The clocks of both parties must be very accurate and be very accurately in time. However, this condition is unacceptable in cellular telecommunication systems: both parties, i.e. the mobile station (MS) and the network do not have access to a clock, that is reliable enough.

When using sequence numbers, each party has to keep track of those sequence numbers that have already been used and are not acceptable any more. The easiest way to implement this is to store the highest sequence number used in MAC calculations so far. This approach has the drawback, that between connections each party must maintain state information which is at least to some level synchronized. That is, they need to store the highest sequence number used so far. This requires the use of a large database at the network side.

A further approach is to include a random number in each message, which the other side must use in MAC calculation when for the next time sending a message, for which MAC authentication is required. This approach has the same drawback as the previous one, i.e. between connections each party must maintain state information, which requires the use of a large database at the network side.

US 5 475 763 by Kaufman et al. (1995) describes a signature system, such as an El Gamal or DSS system, involving the use of long term secret number and a per-message secret number generates the per message secret number without the use of a random number generator or non-volatile storage. The per-message secret number is generated by applying a one-way hash function to a combination of the long term secret number and the message itself.

SUMMARY OF THE INVENTION

An object of the invention is to realize a method for integrity checking, which avoids the problems associated with prior art. A further object of the invention is to provide a method for integrity checking, which does not require storage of state information on the network side.

The objects are reached by using two time-varying parameters in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by

the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.

- 5 The method according to the invention is characterized by that, which is specified in the characterizing part of the independent method claim. The dependent claims describe further advantageous embodiments of the invention.

According to the invention, both parties specify a varying parameter to be used in the generation of MAC values. On the network side in a mobile network, all state
 10 information about the particular user can be discarded after the connection is released. According to the invention, both a sequence number and a network specified value such as a pseudorandom number is used in calculation of the MAC value. In the beginning of the connection, the mobile station determines the initial value used for the sequence counting, and transmits the value to the network. In
 15 addition to the initial value, a counter value is used. The initial value and the counter value are concatenated, added or combined in some other way to produce the parameter to be used in the calculation of the MAC value of a message. One way of combining the two values is using the initial value as the starting value of the counter, which corresponds to the addition of the counter value and the initial value.
 20 The invention does not limit which counter values are used in the inventive method. A suitable value is for example the protocol data unit (PDU) number of the radio link control (RLC) protocol, i.e. the RLC PDU number. Another suitable value is the use of a counter, which is incremented at fixed intervals, for example every 10 milliseconds. Preferably, a counter such as the RLC PDU counter which is already
 25 present in mobile stations and in the network is used in a method according to the invention. Further, also counters associated with ciphering of data over the radio interface can be used in a method according to the invention. Further, the invention does not limit which initial value is used in the inventive method. For example, the current hyperframe number at the time of initiating of the connection can be used as
 30 the initial value. Further, the counter values do not need to be transmitted after the transmission of the initial value, since both sides of the connection can update the counters in the same way during the connection, preserving synchronization. Preferably, when a connection is released, the mobile station stores into its memory the initial value used in the connection or at least the most significant bits of the
 35 initial value, which allows the mobile station to use a different initial value next time. The mobile station can save the information for example in the SIM

(Subscriber Identity Module) card or another memory device, for allowing the mobile station to use a value previously stored in the SIM card of the mobile station in specifying the initial value.

5 The network specifies the random number, or in practice a pseudorandom number in the beginning of the connection. The random number is session specific, i.e. it does not need to be changed within a connection or transmitted to the mobile station more than once in the beginning of the connection, and neither does it need to be stored in the network between connections. Advantageously, the network element generating the random number and taking care of MAC value generation and
10 checking of received messages and MAC values is the radio network controller (RNC). However, the invention is not limited to that, since these functions can be realized in many other network elements as well. The use of RNC is advantageous, since in that case the core network of the cellular telecommunication system does not need to participate in integrity checking of single messages, and since radio
15 access network messaging may also need to be protected by integrity checking.

The invention allows both sides of the connection to perform integrity checking. Since the network specifies a random value in the beginning of the connection, a mobile station of a hostile party cannot successfully perform a replay attack by replaying a message recorded from a previous connection. Since the mobile station
20 specifies the initial value for the connection, replay attacks from a bogus network element operated by a hostile party will not succeed.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in more detail in the following with reference to the accompanying drawings, of which

- 25 Figure 1 illustrates an advantageous embodiment of the invention,
- Figure 2 illustrates a method according to an advantageous embodiment of the invention, and
- Figure 3 illustrates signalling according to an advantageous embodiment of the invention.
- 30 Same reference numerals are used for similar entities in the figures.

DETAILED DESCRIPTION

Figure 1 illustrates a way of calculating the MAC value according to the invention. The IK is the secret integrity key, which is generated during a mobile station authentication procedure in the beginning of a connection. Because the same IK key is used to authenticate many messages possibly even during many consecutive connections, time-varying parameters are needed to avoid hostile attacks during the connection. For that purpose, a counter value COUNT and a random value RANDOM are used in the MAC calculation as well. According to the invention, a message 1 and the IK, COUNT, and RANDOM values are input into a calculation means 10, which calculates a MAC value according to the inputs and the particular authentication algorithm. We note here, that the invention is not limited to any specific way of calculating the MAC value from the inputs illustrated in figure 1. The invention is not limited to any specific lengths of the input values. For example, for the UMTS (Universal Mobile Telecommunication System) cellular system suitable lengths are 128 bits for the IK value, 32 bits for the COUNT value, 32 bits for the RANDOM value, and 16 bits for the MAC value. However, other lengths could be used even for the UMTS system, and other inputs can be used in addition to these values.

If a new IK value is generated in an authentication process in the beginning of the current connection, the mobile station can reset the initial value of COUNT, since new IK value provides security against replay attacks. The storing of the initial value or a part of it for use with the next connection is necessary, since the IK value might not change, when the next connection is established. This is very probable for example when using a multifunction mobile station in the UMTS system, since the mobile station can have multiple simultaneous connections of various types, and establish and release new connections during a single communication session. The network does not necessarily perform full authentication for each new connection, whereby the mobile station will not always receive a new IK value for each new connection. However, when the IK is changed, the mobile station can reset the initial COUNT values without danger of compromising security.

Figure 2 illustrates a method according to an advantageous embodiment of the invention. Figure 2 illustrates a method for integrity checking of a message transmitted during a connection between a cellular telecommunication network and a mobile station.

In the first step 50, the transmitting party calculates the authentication value (MAC) of the message on the basis of the message, a first value specified by the network, said first value being valid for one connection only, a second value specified at least in part by the network, and a third value at least partly specified by the mobile station. Preferably, said first value is a pseudorandom value such as the RANDOM value described previously. Further, said third value is preferably a counter value such as the COUNT value described previously, which value is incremented during the connection. For example, the RLC PDU value can be used for generation of the COUNT value. As described previously, the mobile station specifies an initial value for the counter value in the beginning of the connection. The initial value can be used as a starting value for a counter producing the COUNT values, or the initial value can be combined with some other counter value such as the RLC PDU value for producing said third value.

In the next step 52, the message is transmitted from the transmitting party to the receiving party, which calculates a second MAC value as described previously, and compares the received MAC value and the calculated MAC value in step 56. If they are found to be equal, the message is accepted in step 58, and if they are found to be unequal, the message is rejected in step 60. In the case of uplink messaging, the steps of calculation 54 and comparison 56 can advantageously be performed by a radio network controller in the cellular telecommunication network. The method of figure 2 is used for checking the integrity of at least some of uplink and downlink messages.

Figure 3 illustrates one example of how to initiate a connection according to an advantageous embodiment of the invention. Figure 3 shows an advantageous solution to the problem of how to exchange two initial values for the purposes of integrity checking. We note here that the signalling sequence shown in figure 3 is in no way limited to passing only the COUNT and RANDOM values described previously. Signalling according to figure 3 can be used for exchange of any two keys in the beginning of a connection. Figure 3 shows as an example signalling associated with a mobile originated call, but corresponding signalling sequences can be used also in other situations, such as in establishing a mobile terminating call, or in a paging response procedure.

Figure 3 shows a particular example of a method according to the invention. The central idea in figure 3 is, that the RNC stores the message or messages received from the mobile station and authenticated with a MAC value until the time, when it is able to check the MAC value of the message(s). If one or all of the MAC values

are later found to be false, the network can then decide, if it should discard the initiated connection.

Figure 3 illustrates signalling between a mobile station MS 20, a radio network controller RNC 30, and core network CN 40 in a situation, in which the mobile station initiates a connection. Figure 3 illustrates the signalling using terminology of the UMTS system. In the first step 100, the mobile station sends the initial connection request message RRC SETUP REQ to the network. After receiving the connection request message, the RNC generates the RANDOM value, after which the RNC replies by sending 105 an acknowledgment message ACK to the mobile station. The RNC specifies the RANDOM value to the mobile station by attaching the value as a parameter to the ACK message, which is shown in figure 3 by the label RANDOM appearing under the arrow 105. After receiving the acknowledgment and the RANDOM value, the mobile station needs to send the initial COUNT value to the network. This can be realized basically in two ways: by defining a new message for that purpose, for example in the RRC level, or by attaching the COUNT value as a parameter to an existing message. Arrow 110 denotes the former approach, i.e. denotes a message specifically defined for transmitting the COUNT value. Arrow 115 denotes the latter approach, i.e. attaching the COUNT value as a parameter to an existing message. In the example of figure 3, the existing message is a CM SERV REQ message. Further, also an IK key identification number may be transmitted as a parameter to the message. During an authentication process in which an IK is generated, each IK is assigned an identification number, whereafter the MS and the network may refer to the IK simply by using the identification number.

In the example of figure 3, the mobile station sends a classmark service request message CM SERV REQ to the network, specifying a temporary identifier TMSI and a capability class identifier CM2 to the network. If a specific message was not used to transport the initial COUNT value to the network, the initial COUNT value is passed to the network as a further parameter to the CM SERV REQ message. Further, the mobile station transmits a MAC value calculated on the basis of the COUNT and RANDOM values, and an IK value received and stored during a previous connection. Upon receiving the message, the RNC removes and stores the MAC value from the message as well as the possibly existing COUNT value, and forwards 120 the rest of the message to the core network. The RNC stores the whole message as well for later use, which will be described later. According to UMTS specifications, the core network may perform an authentication procedure at this

stage, which is represented by arrows 125 and 130 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages.

5 The next step depends on whether the network has an IK value for the mobile station or not. If the network performed the authentication in steps 125 and 130, the network has the IK value determined in the authentication. Alternatively, the network may have an old IK value stored in relation to a previous connection. The IK value is stored in the core network registers. If the network has an IK value, the method continues at step 135; if not, at step 150. This is represented by step 132 and
10 the associated dashed arrow in figure 3.

In step 135, the core network sends a ciphering mode CIPH MODE message to the RNC, attaching the ciphering key CK and the IK value as parameters to the message. With this message, the CN supplies the IK value to the RNC, which was previously unaware of the IK value, if the authentication procedure was not
15 performed at steps 125 and 130. At this stage, the RNC is able to check the CM SERV REQ message stored at step 115, since it now has the COUNT, the RANDOM, and the IK values necessary for calculating the MAC value of the message. The RNC calculates a MAC value and compares 137 it to the MAC value stored previously at step 115. If the match, the method continues at step 140. If they
20 do not match, the method continues at step 160.

In step 140, the RNC sends to the MS a CIPHERING COMMAND message to start ciphering, to which the MS replies 145 by sending a ciphering response message CIPHERING RSP back to RNC. After that, the communication continues normally, and the continuation is not depicted in figure 3.

25 In step 150, the network performs an authentication process, which is represented by arrows 150 and 155 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages. After that, the core network informs the RNC about the new IK (not shown).

30 At this stage the RNC needs to make sure, that the MS is the correct one and can calculate the MAC values accordingly. The RNC can perform for example a classmark request procedure or some other suitable procedure to that effect. That is, the RNC sends 160 a classmark request CLASSMARK REQ message to the MS, which replies by sending 165 a response message RSP back to the RNC, attaching the classmark information CM2 as a parameter to the message, and the calculated

MAC value at the end of the message. Now the RNC can again check the MAC, and if no hostile party has replayed any of the previous messages, the MAC values calculated by the RNC and the MS will match, since the three key values IK, RANDOM, and COUNT are now known both to the MS and the RNC. After
 5 receiving the classmark response message RSP, the RNC sends 170 the classmark information in a CLASSMARK message to the core network, as required by the UMTS specifications.

Although in the previous description, the network is described to specify a random number to be used as the network-specified varying parameter, also other than
 10 random values can be used. For example, although being a less advantageous example of an embodiment of the invention, the network may use a counter value, and store the counter value in a central register in order to be able to use a different value during the next connection. Naturally, this embodiment has the disadvantage
 15 of the burden of storage of the values of the users to be used in the following connections.

In the previous examples, the invention has been described in relation to a cellular telecommunication system. The invention can be very advantageously used in such a system, since it requires very little messaging, and thus uses only a diminutive amount of valuable air interface resources. However, the invention can be applied
 20 also in other communication systems.

The invention has several advantages. For example, according to most advantageous embodiments there is no need for maintaining synchronized state information between different connections. That is, these embodiments do not require the network to store any counter information for effecting the integrity checking which
 25 is a considerable advantage, since such storage would have to be effected in a central register such as the VLR (Visitor Location Register) or the HLR (Home Location Register). According to these most advantageous embodiments, all state information about the connection can be discarded on the network side in a mobile network after the connection is released. The invention allows the integrity checking
 30 to be performed by a network element outside the core network, such as the RNC in the case the UMTS cellular system.

The invention does not specify any upper limit for the number of values used in calculation of MAC values. Any other values in addition to those described for example in relation to figure 1 may be used as well. Further, the invention does not

limit, which messages are subjected to integrity checking: all messages, a certain group of messages, or messages selected in some other way.

5 The name of a given functional entity, such as the radio network controller, is often different in the context of different cellular telecommunication systems. For example, in the GSM system the functional entity corresponding to a radio network controller (RNC) is the base station controller (BSC). Therefore, the term radio network controller is intended to cover all corresponding functional entities regardless of the term used for the entity in the particular cellular telecommunication system. Further, the various message names such as the RRC SETUP REQ message
10 name are intended to be examples only, and the invention is not limited to using the message names recited in this specification.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention. While a preferred embodiment of the invention has been described in detail, it should be
15 apparent that many modifications and variations thereto are possible, all of which fall within the true spirit and scope of the invention.

Claims

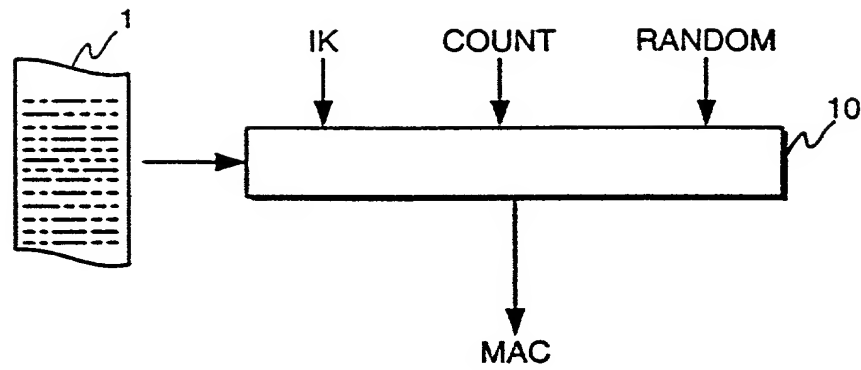
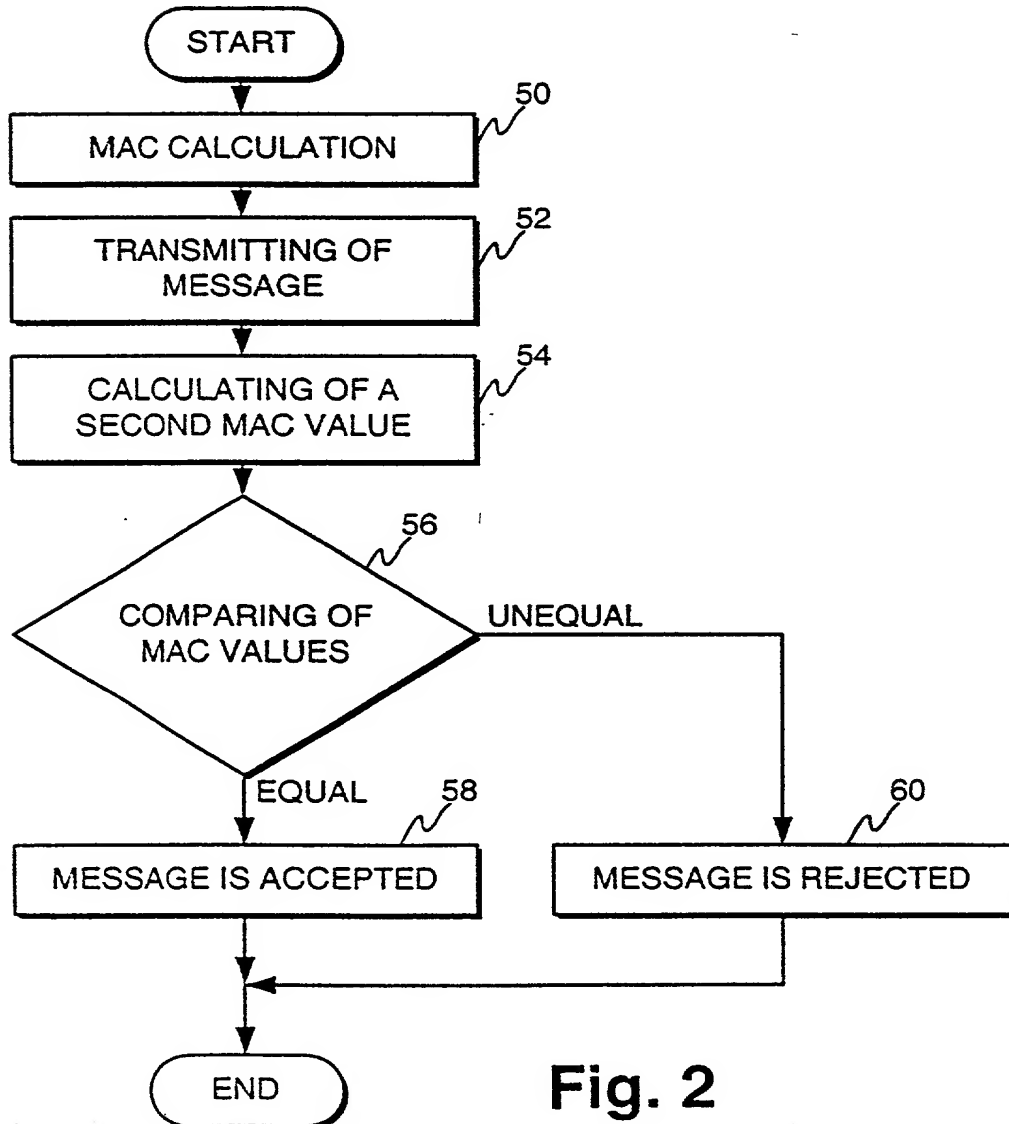
1. Method for integrity checking of messages transmitted during a connection between a first party and a second party, in which method an authentication value is calculated for a message,
- 5 **characterized** in that the method comprises steps, in which the authentication value of a message is calculated on the basis of
 - the message,
 - a first value specified by the first party, said first value being valid for one connection only,
 - 10 - a counter value at least partly specified by the second party.
2. A method according to claim 1, **characterized** in that said first party is a cellular telecommunication network and said second party is a mobile station.
3. A method according to claim 1, **characterized** in that the authentication value of a message is calculated (54) also on the basis of a second value specified at least
 15 in part by the first party.
4. A method according to claim 1, **characterized** in that said first value is a pseudorandom value.
5. A method according to claim 2, **characterized** in that the mobile station specifies an initial value for the counter value.
- 20 6. A method according to claim 2, **characterized** in that the mobile station specifies an initial value which is combined with a counter value for producing a third value.
7. A method according to claim 5, **characterized** in that the mobile station uses a value previously stored in the SIM card of the mobile station in specifying said
 25 initial value.
8. A method according to claim 1, **characterized** in that said cellular telecommunication network is an UMTS network, and said first value is specified by a radio network controller.

Abstract

The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Two time-varying parameters are used in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.

Fig. 1

1 / 2

**Fig. 1****Fig. 2**

2 / 2

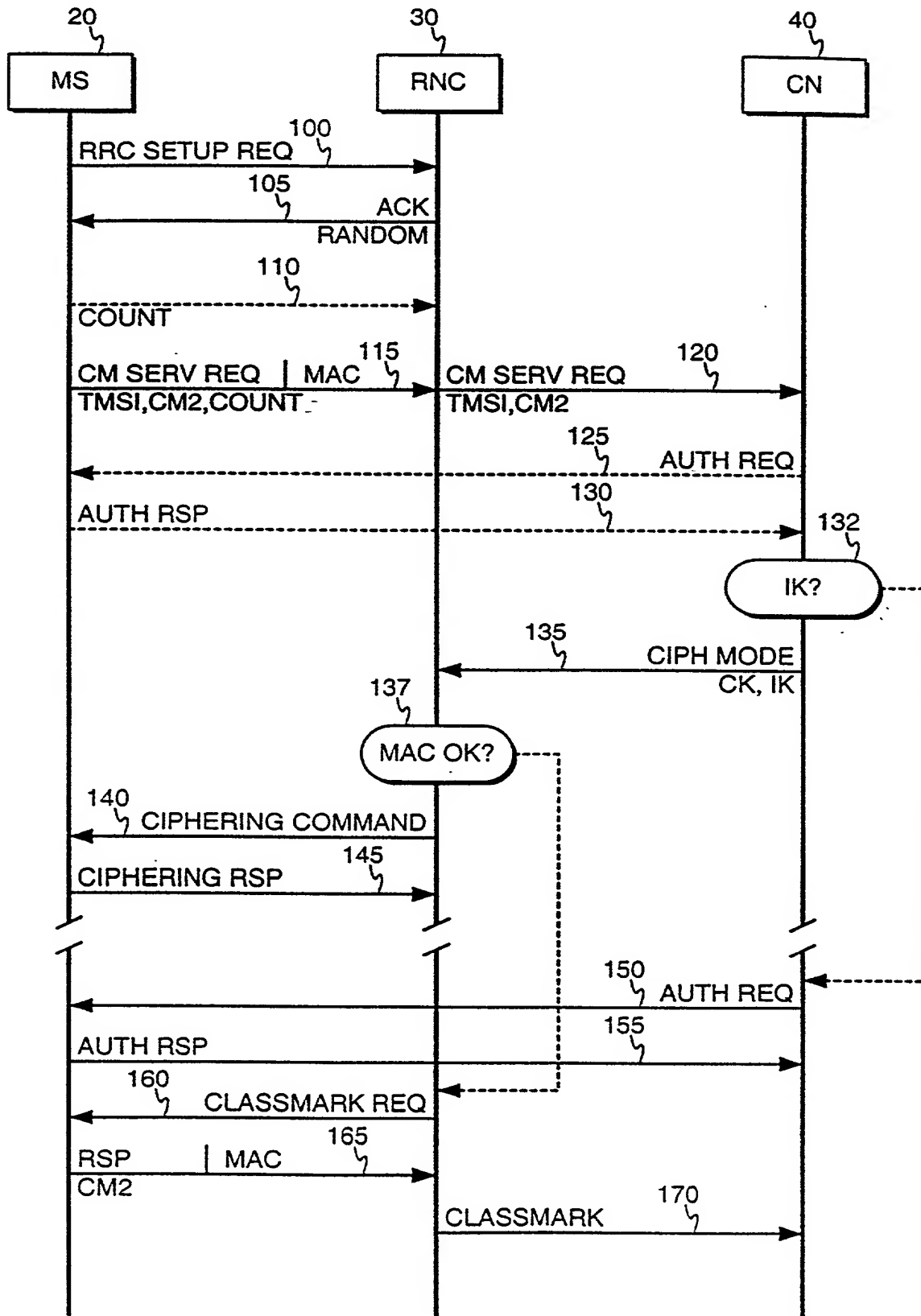


Fig. 3

Combined Declaration for Patent Application and Power of Attorney (Continued)
(Includes Reference to PCT International Applications)

Attorney's Docket No.
4925-158PUS

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. SERIAL NUMBERS ASSIGNED (if any)		
PCT/FI00/00421	11 May 2000		x	

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (*List name and registration number*)

MYRON COHEN, Reg. No. 17,358; THOMAS C. PONTANI, Reg. No. 29,763; LANCE J. LIEBERMAN, Reg. No. 28,437; MARTIN B. PAVANE, Reg. No. 28,337; MICHAEL C. STUART, Reg. No. 35,698; KLAUS P. STOFFEL, Reg. No. 31,668; EDWARD M. WEISZ, Reg. No. 37,257; JULIA S. KIM, Reg. No. 36,567; VINCENT M. FAZZARI, Reg. No. 26,879; ALFRED W. FRÖEBRICH, Reg. No. 38,887; KENT H. CHENG, Reg. No. 33,849; ROGER S. THOMPSON, Reg. No. 29,594; F. BRICE FALLER, Reg. No. 29,532; YUNLING REN, Reg. No. 47,019; DAVID J. ROSENBLUM, Reg. No. 37,709; ELI WEISS, Reg. No. 17,765; TONY CHEN, Reg. No. 44,607.

Send correspondence to:

Michael C. Stuart

Reg. 35,698

Cohen, Pontani, Lieberman & Pavane

551 Fifth Avenue, Suite 1210

New York, New York 10176




Direct Telephone calls to:
(name and telephone number)

Michael C. Stuart
(212) 687-2770

201	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	<u>Valtteri</u>	<u>NIEMI</u>	<u>Valtteri</u>	
	RESIDENCE, CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
		<u>Helsinki</u>	<u>Finland</u> <u>FIX</u>	<u>Finland</u>
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
		<u>Itämerenkatu 11-13</u>	<u>Helsinki</u>	<u>FIN-00180 Finland</u>
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	<u>Jaakko</u>	<u>RAJANIEMI</u>	<u>Jaakko</u>	
	RESIDENCE, CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
		<u>Helsinki</u>	<u>Finland</u> <u>FIX</u>	<u>Finland</u>
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
		<u>Lapinrinne 2 A 11</u>	<u>Helsinki</u>	<u>FIN-00180 Finland</u>

Attorney's Docket No.
4925-158PUS

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201 	SIGNATURE OF INVENTOR 202 	SIGNATURE OF INVENTOR 203 
DATE 11/15/2001	DATE 11/16/2001	DATE 11/13/2001

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

INTEGRITY PROTECTION METHOD FOR RADIO NETWORK SIGNALING

the specification of which (check only one item below)

☐ is attached hereto

☐ was filed as United States application

Serial No. _

on _

and was amended

on _ (if applicable).

☒ was filed as PCT international application

Number PCT/FI00/00421

on 11 May 2000

and was amended under PCT Article 19

on _ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of the application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

PRIOR FOREIGN/PCT APPLICATIONS AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

Country (if PCT, indicate "PCT")	Application Number	Date of Filing (day, month, year)	Priority Claimed Under 35 U.S.C. 119	
Finland	991088	11 May 1999	<input checked="" type="checkbox"/> YES	<input type="checkbox"/> NO
PCT	PCT/FI00/00421	11 May 2000	<input checked="" type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO
			<input type="checkbox"/> YES	<input type="checkbox"/> NO